Integrazione di ISE 3.3 con JAMF come server MDM

Sommario

Introduzione

Questo documento descrive le procedure necessarie per implementare Identity Services Engine v3.3 con l'istanza 10.48.X di JAMF PRO.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE)
- JAMF come soluzione MDM

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Cisco Identity Services Engine (ISE) v3.3
- JAMF PRO v10.48.1-t1689600654

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

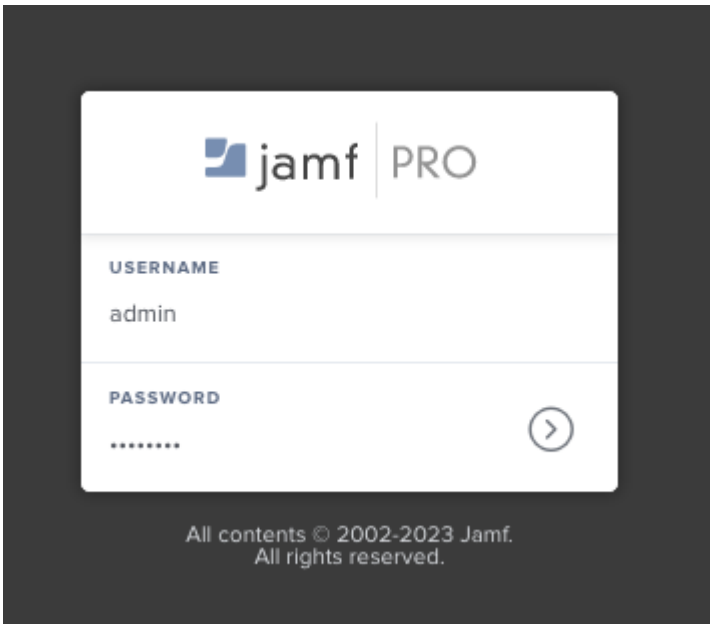
Cisco ISE supporta JAMF come server MDM per la gestione di computer Windows. Quando questi computer (gestiti da JAMF) sono connessi e autenticati, ISE recupera le informazioni di conformità dai server JAMF per recuperare ulteriori informazioni sulla postura di sicurezza di tali dispositivi.

Utilizza le informazioni per applicare la sicurezza dell'accesso, consentendo/negando l'accesso a questi computer, a seconda dei criteri e delle condizioni configurate in ISE. Pertanto, questa implementazione aiuta a identificare potenziali vulnerabilità e debolezze della sicurezza che potrebbero essere sfruttate dagli aggressori.

Configurazione

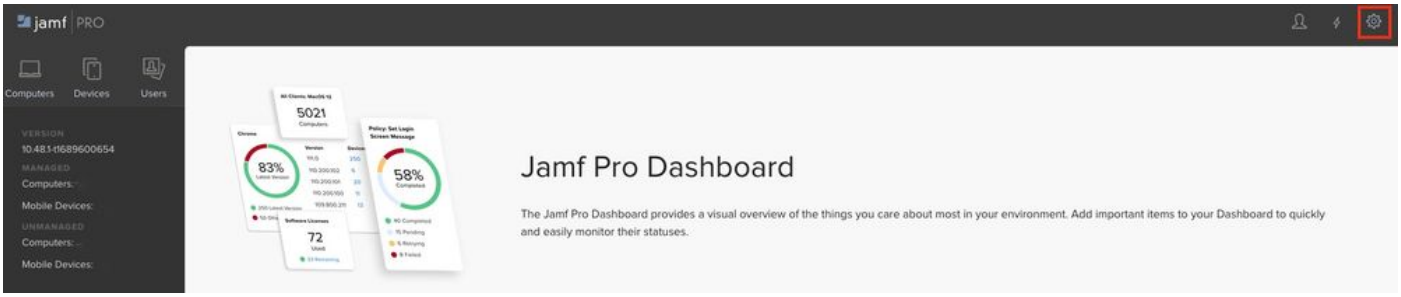
Preparazione di JAMF PRO per la connessione MDM

Passaggio 1. Accedere con il cloud JAMF con l'account per i privilegi di amministratore all'indirizzo: https://YOUR_ACCOUNT.jamfcloud.com/index.html.



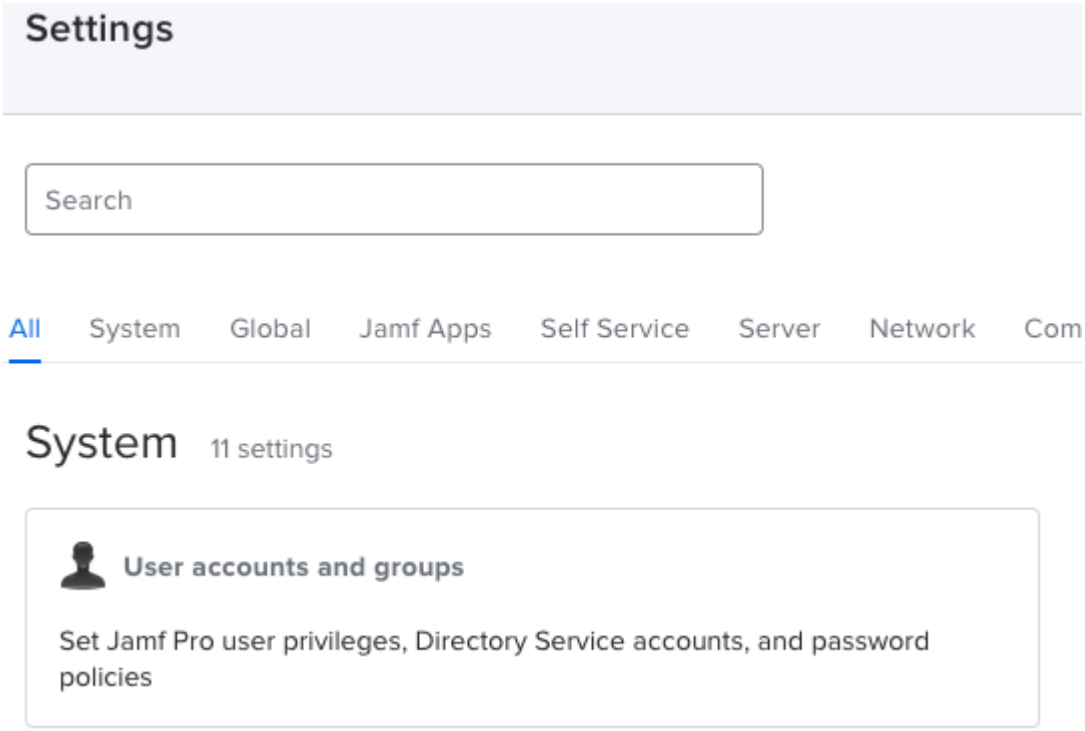
Pagina di accesso JAMF PRO

Passo 2. Dal menu principale, selezionare l'icona ingranaggio.



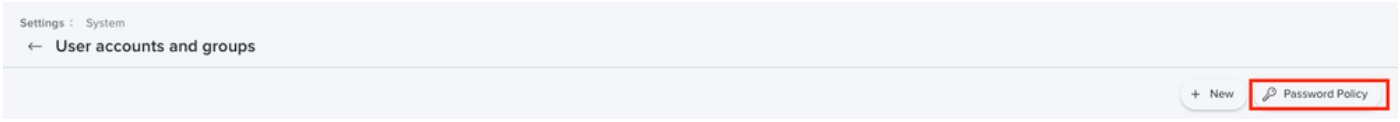
Dashboard JAMF PRO

Passaggio 3. Nel menu principale, scegliere Sistema > Account utente e gruppi.



Impostazioni di sistema di JAMF PRO

Passaggio 4. Selezionare l'opzione Criteri password.



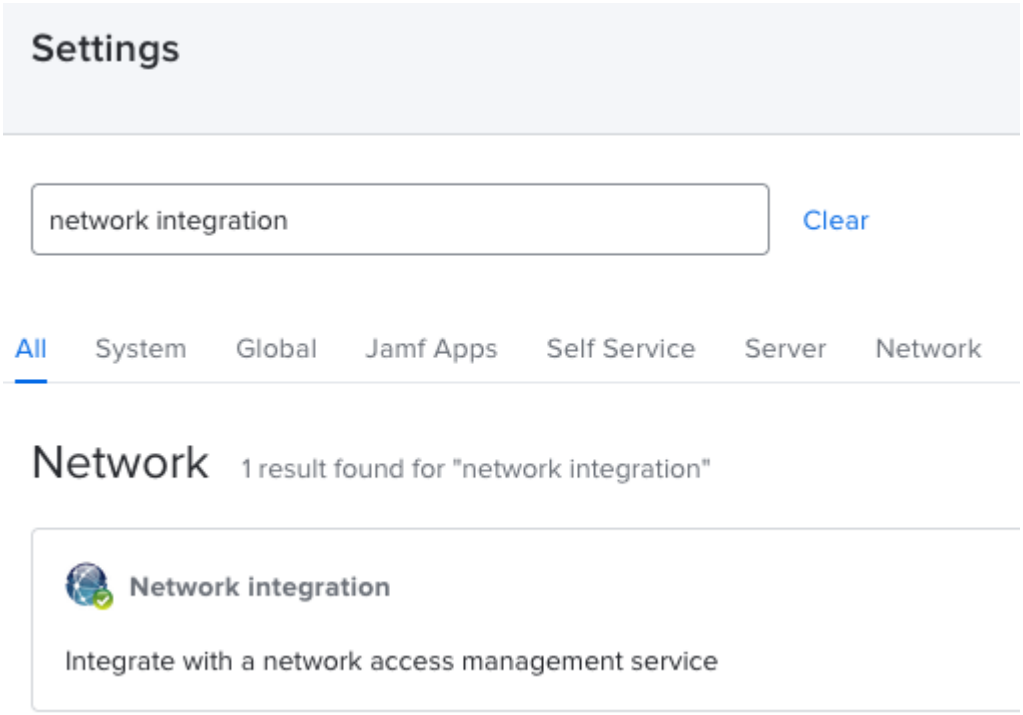
Account e gruppi di utenti JAMF PRO

Passaggio 5. In questa sezione, confermare di avere l'opzione Allow Basic Authentication (Consenti autenticazione di base) oltre a Bearer Token Authentication (Autenticazione token bearer).

Nota: A partire da JAMF PRO v10.35, l'autenticazione di base per l'API non è abilitata per impostazione predefinita. Pertanto, è necessario attivare queste funzionalità per garantire il funzionamento dell'integrazione MDM.

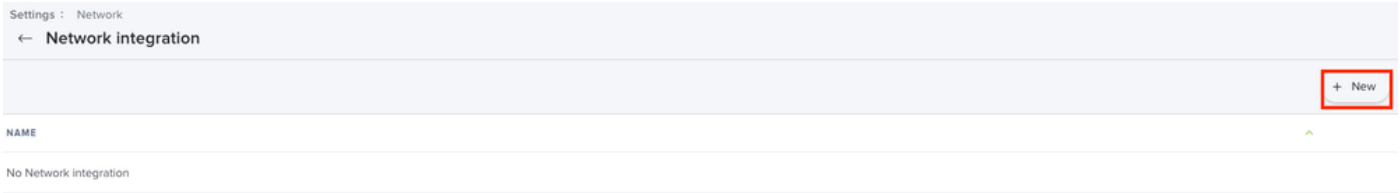
Per ulteriori informazioni, vedere Modifiche all'autenticazione API classica.

Passaggio 6. Dopo aver abilitato l'ultima funzionalità, andare alla pagina Impostazioni menu descritta al passaggio 3, cercare Network IntegrationMenu e selezionarla.



Integrazione di rete JAMF PRO

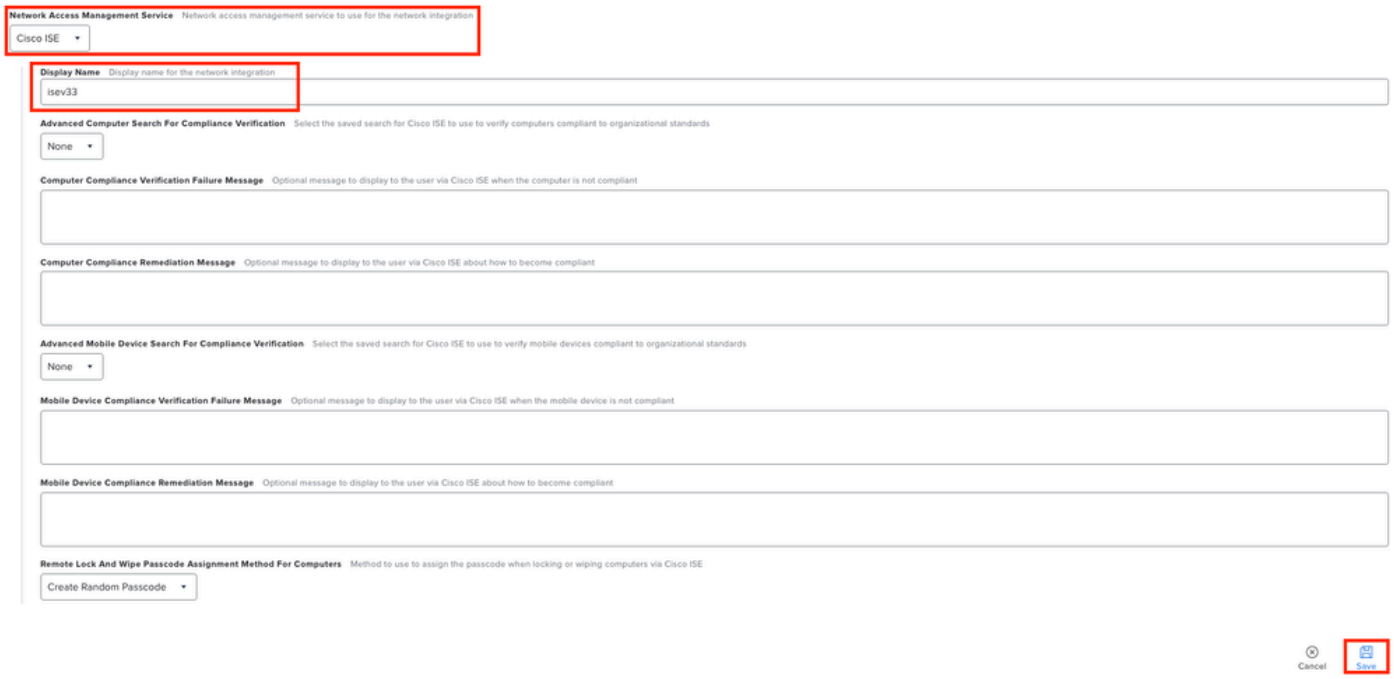
Passaggio 7. Procedere a selezionare + Nuovo per aggiungere una nuova istanza per ISE 3.3.



Impostazioni di integrazione di rete JAMF PRO

Passaggio 8. Nel menu a discesa in Network Access Management Service, lasciare l'opzione contrassegnata come Cisco ISE.

- Specificare quindi un nome nel menu Display Name (Nome visualizzato) come illustrato nell'esempio.
- Per le impostazioni iniziali e la connessione per ISE, la configurazione può essere lasciata con queste configurazioni standard.
- Continuare con il salvataggio della configurazione.

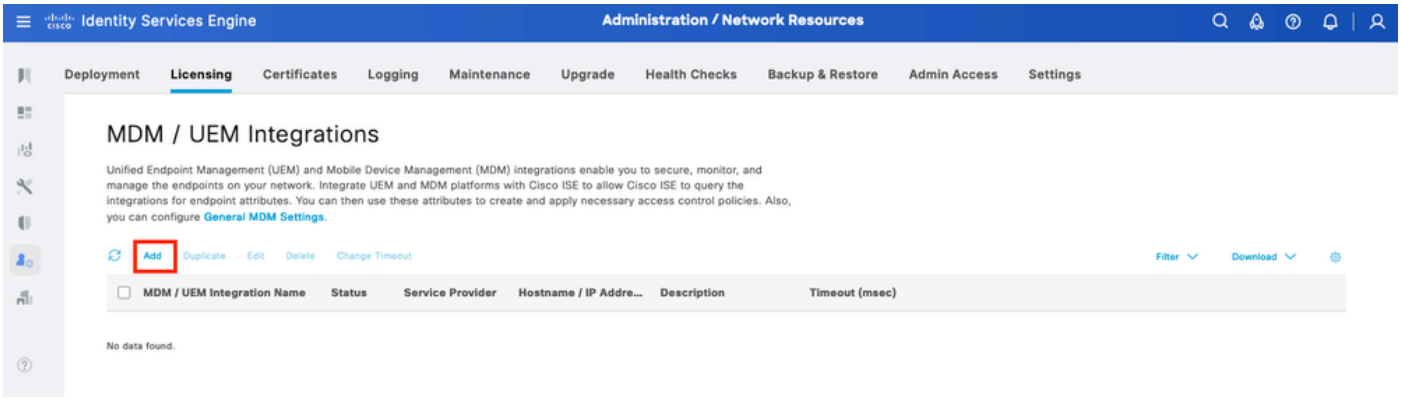


Esempio di configurazione Integrazione in rete con ISE

Passaggio 9. L'integrazione genera un URL di integrazione di rete nel formato seguente: https://YOUR_ACCOUNT.jamfcloud.com/networkIntegrationEndpoint/ID. Salvare l'URL perché sarà necessario utilizzarlo in un secondo momento per connettersi ad ISE.

Preparazione di ISE per la connessione MDM

Passaggio 1. Selezionare Menu > Amministrazione > Risorse di rete > MDM esterno, quindi fare clic su Aggiungi.

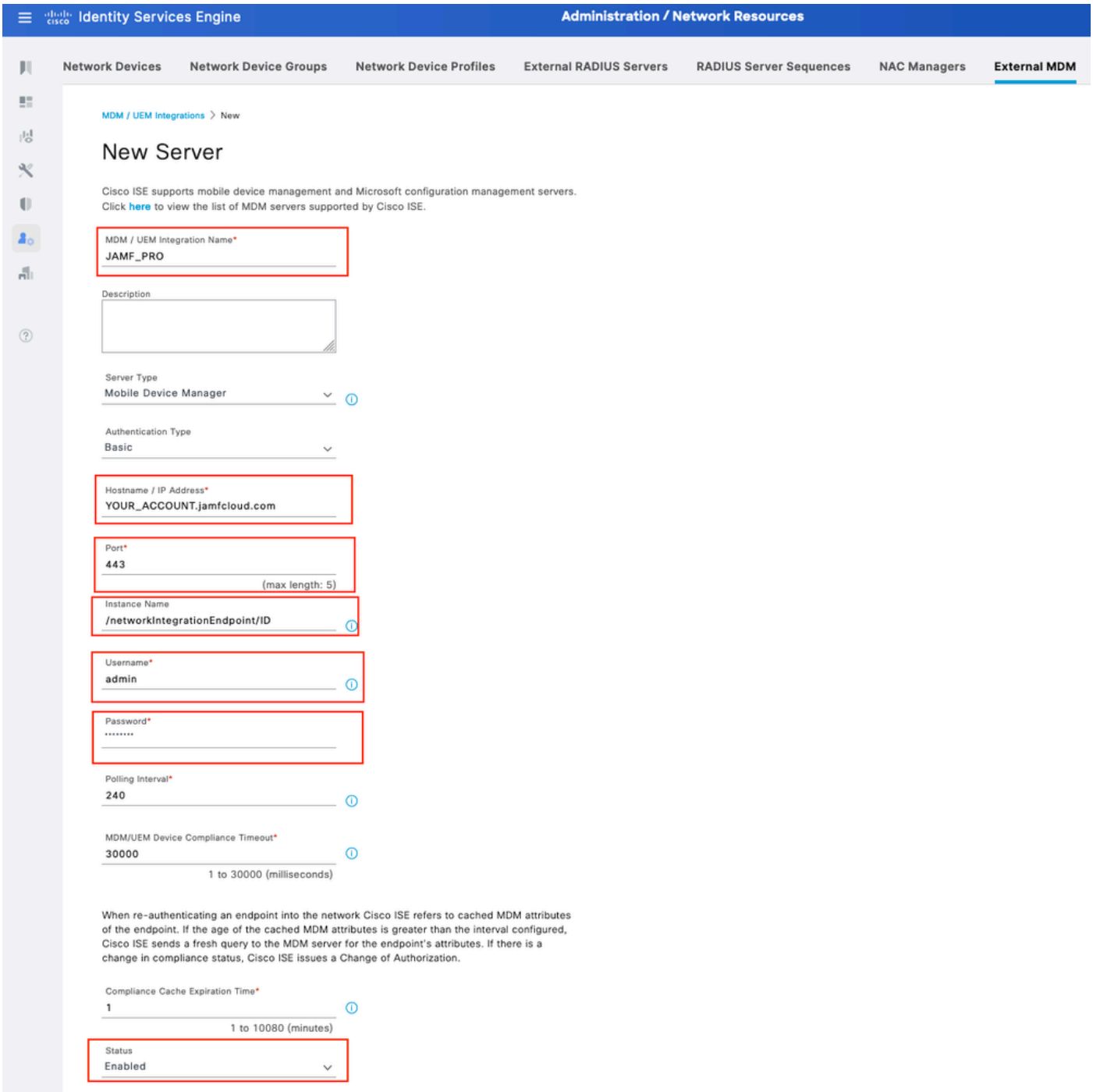


Menu ISE MDM integration

Passaggio 2. Assegnare un nome all'installazione nel segmento MDM/UEM Integration Name.

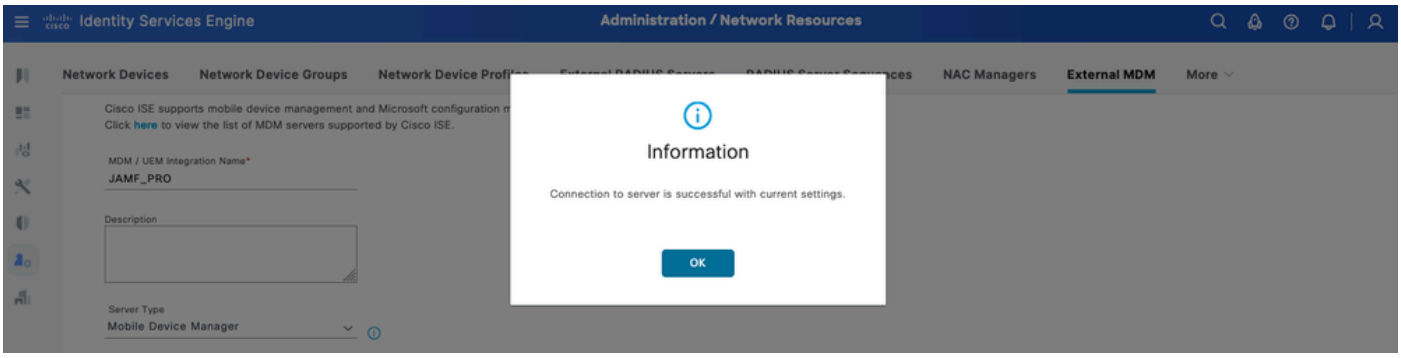
- Nella sezione Nome host / Indirizzo IP selezionare YOUR_ACCOUNT.jamfcloud.com dall'URL generato nei passaggi precedenti.

- In Porta, selezionare la porta 443 per la connessione HTTPS con l'istanza JAMF PRO.
- Nella sezione Nome istanza, immettere i valori senza la sezione nell'URL creato (in questo caso: /networkIntegrationEndpoint/ID).
- Immettere un nome utente con accesso completo all'istanza JAMF PRO insieme alla password corrispondente.
- Modificare lo stato del server MDM in Abilitato.



Esempio di configurazione di ISE MDM JAMF PRO

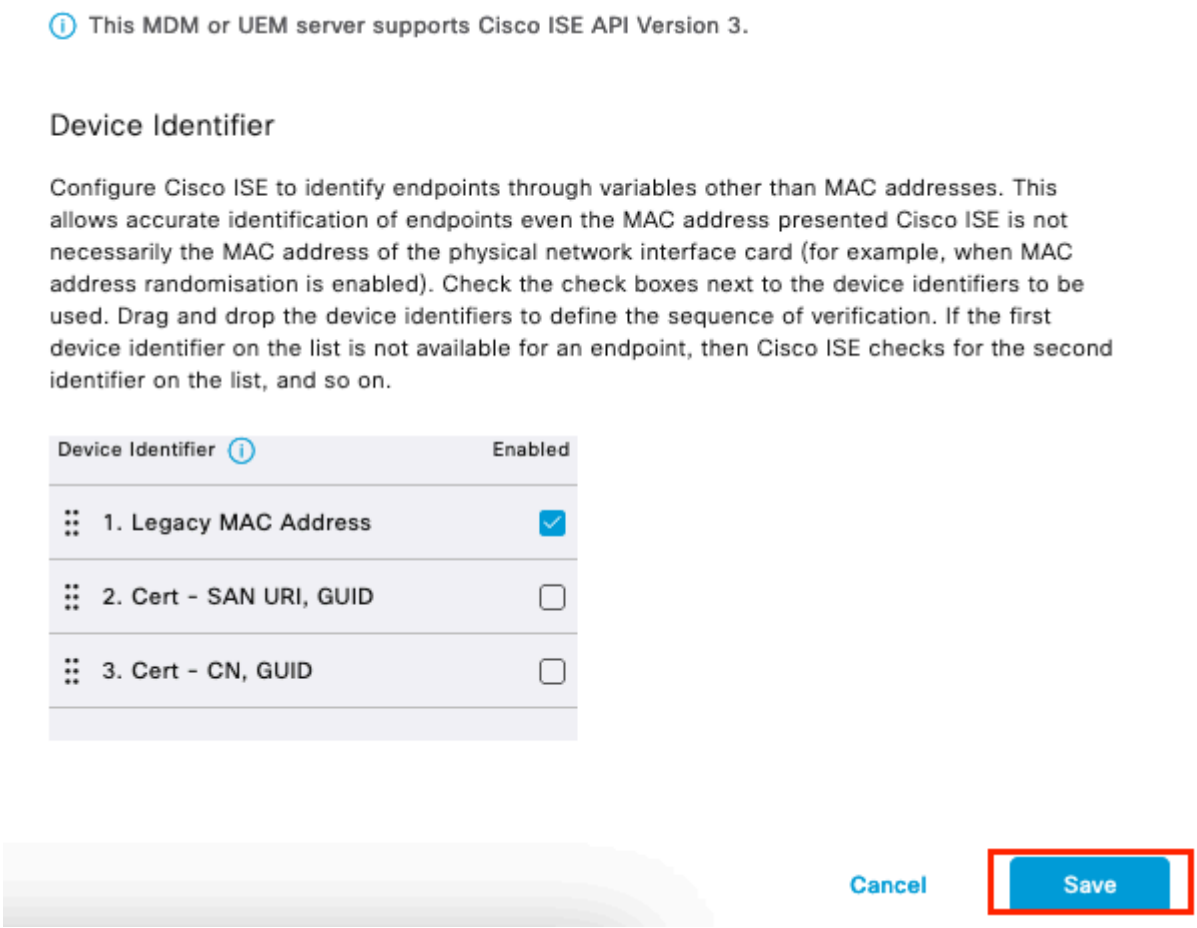
Passaggio 3. Scorrere verso il basso e passare a Test connessione. Se la connessione ha esito positivo, viene visualizzata questa immagine. Se non si riceve lo stesso output, consultare la sezione Risoluzione dei problemi in questo documento.



Connessione all'account JAMF MDM riuscita

Passaggio 4. Selezionare OK nell'opzione precedente. In fondo alla pagina, individuare l'identificatore del dispositivo a cui l'ISE è associato alla sessione dell'endpoint.

- A seconda dello scenario, è possibile selezionare l'indirizzo MAC del dispositivo o gli attributi del certificato.
- Dopo aver personalizzato la sezione, salvare la configurazione.



Configurazione aggiuntiva per il server MDM

Verificare la connettività iniziale dell'integrazione con l'istanza JAMF PRO.

Acquisizione pacchetti: Se la connettività ha esito positivo, è possibile visualizzare il traffico HTTPS inviato dal server PAN ISE all'istanza JAMF PRO:

Protocol	Length	Info
TCP	74	47386 → 3128 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=211264130 TSecr=0 WS=128
TCP	74	3128 → 47386 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=503104063 TSecr=211264130 WS=128
TCP	66	47386 → 3128 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=211264131 TSecr=503104063
HTTP	183	CONNECT [redacted] 443 HTTP/1.1
TCP	66	3128 → 47386 [ACK] Seq=1 Ack=118 Win=65152 Len=0 TSval=503104064 TSecr=211264131
HTTP	105	HTTP/1.1 200 Connection established
TCP	66	47386 → 3128 [ACK] Seq=118 Ack=40 Win=29312 Len=0 TSval=211264384 TSecr=503104317
TLSv1…	387	Client Hello
TCP	66	3128 → 47386 [ACK] Seq=40 Ack=439 Win=64896 Len=0 TSval=503104318 TSecr=211264385
TLSv1…	166	Server Hello
TCP	1254	3128 → 47386 [PSH, ACK] Seq=140 Ack=439 Win=64896 Len=1188 TSval=503104457 TSecr=211264385 [TCP segment of a reassembled PDU]
TCP	66	47386 → 3128 [ACK] Seq=439 Ack=1328 Win=32128 Len=0 TSval=211264524 TSecr=503104457
TCP	1254	3128 → 47386 [PSH, ACK] Seq=1328 Ack=439 Win=64896 Len=1188 TSval=503104457 TSecr=211264385 [TCP segment of a reassembled PDU]
TLSv1…	2641	Certificate
TCP	66	47386 → 3128 [ACK] Seq=439 Ack=5091 Win=40192 Len=0 TSval=211264525 TSecr=503104457
TLSv1…	413	Server Key Exchange, Server Hello Done
TLSv1…	141	Client Key Exchange
TCP	66	3128 → 47386 [ACK] Seq=5438 Ack=514 Win=64896 Len=0 TSval=503104459 TSecr=211264526
TLSv1…	72	Change Cipher Spec
TLSv1…	111	Encrypted Handshake Message
TCP	66	3128 → 47386 [ACK] Seq=5438 Ack=520 Win=64896 Len=0 TSval=503104462 TSecr=211264529
TCP	66	3128 → 47386 [ACK] Seq=5438 Ack=565 Win=64896 Len=0 TSval=503104463 TSecr=211264529
TLSv1…	117	Change Cipher Spec, Encrypted Handshake Message
TLSv1…	360	Application Data
TCP	66	3128 → 47386 [ACK] Seq=5489 Ack=859 Win=64640 Len=0 TSval=503104601 TSecr=211264668
TLSv1…	1617	Application Data, Application Data
TCP	66	47386 → 3128 [ACK] Seq=859 Ack=7040 Win=46208 Len=0 TSval=211264922 TSecr=503104855

Esempio di acquisizione di pacchetti di connettività con l'istanza JAMF

Logs on ISE: ISE elabora e analizza i dati di conseguenza, come mostrato nel file ise-psc.log:

```
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::- inside the method : callMdmSer
TRACE [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- Inside MDMVerifyServer.veri
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- apiVersionSb : 3, mdmApiVer
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- MDM Rest API Server Query S
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- MDM Rest API Server Query P
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- 1. Connecting to the MDM se
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDom: start  HTTP r
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDomNonComp: start
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- ===mdmFlowInfo===null,=====serve
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- QueryType is heartbeatQuery
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- using httpClient for http query
INFO  [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- GET: MDM Server URL: https://YOU
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- Proxy Config in request  = [,PRO
.
.
INFO  [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- MDM Server Response Code: 200
TRACE [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::-
Response data received from the MDM server : <?xml version="1.0" encoding="UTF-8"?><ise_api><name>mdmin
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDom: end  HTTP req
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDomNonComp: end  H
TRACE [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- isMdmSettingsIdNotNull flag
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::- returning from the method : ca
  apiPath: /ID/ciscoise/v3
```

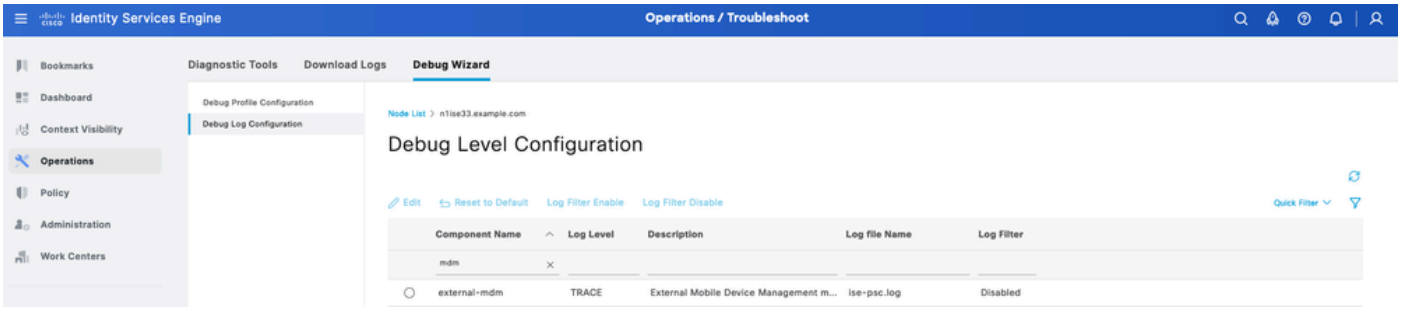
```
  redirectUrl: https://YOUR_ACCOUNT.jamfcloud.com/enroll
  queryMaxSize: 1000
  apiVersion: 3
  vendor: JAMF Software
  productName: JSS
  productVersion: 10.48.1-t1689600654
  COMMA: ,
  errorMsg: null
  errorOccurred: false
}
```

Impossibile raggiungere il server MDM

La base di questa integrazione è costituita dalle query che ISE esegue periodicamente sull'istanza JAMF-PRO. Il punto di riferimento in cui viene eseguita la risoluzione dei problemi (in questa istanza) è il PAN (Primary Administration Node). Nel nodo PAN il metodo di connettività è configurato per raggiungere il server MDM. Questo stesso metodo viene replicato in tutti i nodi per l'implementazione.

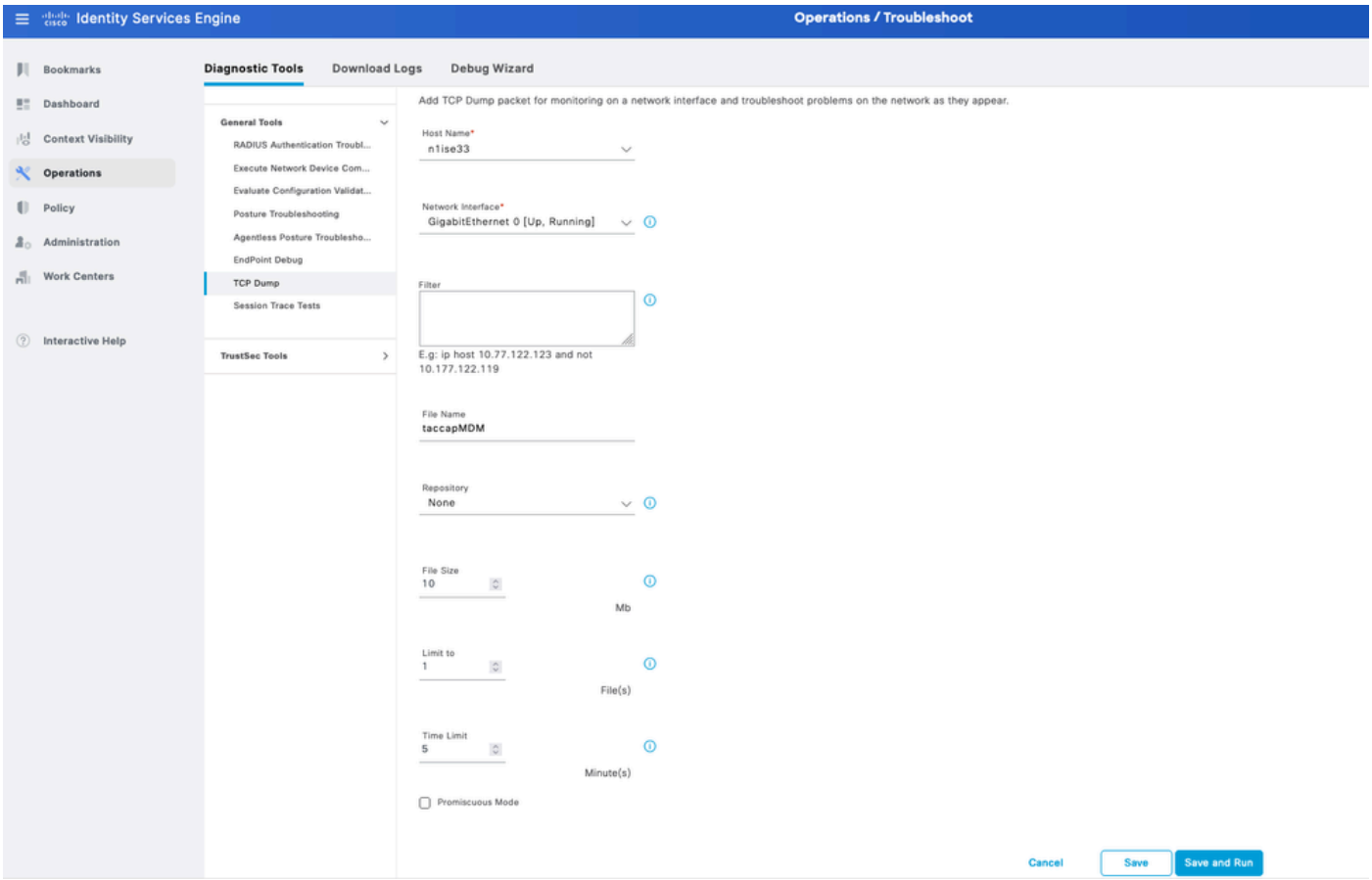
Per risolvere i problemi di raggiungibilità, è possibile seguire la procedura descritta di seguito.

Passaggio 1. Abilitare il componente external-mdm a livello TRACE sul nodo PAN.



Componente MDM esterno a livello TRACE per la risoluzione dei problemi

Passaggio 2. Impostare un'acquisizione dal nodo PAN e salvare la configurazione.



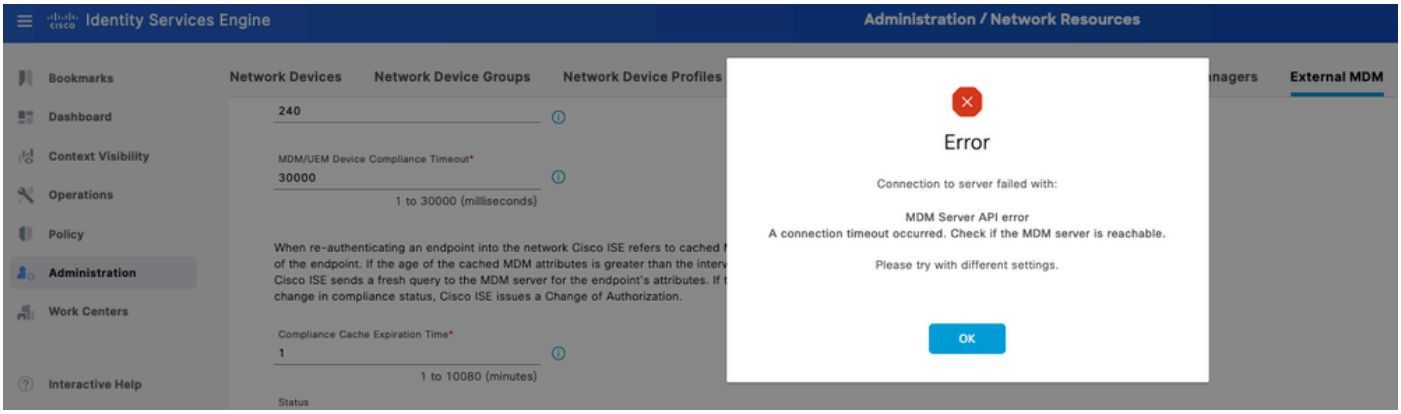
Esempio di acquisizione di pacchetti per raccogliere informazioni sulla connessione MDM

Passaggio 3. Spostarsi nel menu MDM esterno. Eseguire l'acquisizione dal passaggio 2 e selezionare il pulsante Test connessione. Attendere che venga visualizzato l'errore.

Passaggio 4. Interrompere l'acquisizione dal passaggio 2. Esaminare i log corrispondenti a ise-psc.log per analizzare il comportamento.

Scenario 1. Timeout Della Connessione

Nello scenario, quando si riceve questo errore in ISE durante il test della connessione con JAMF:



I log relativi a MDM esterno rivelano queste informazioni:

```
TRACE [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- Inside MDMVerifyServer.veri
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- API version retrieved from
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- apiVersionSb : 3, mdmApiVer
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- MDM Rest API Server Query S
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- MDM Rest API Server Query P
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- 1. Connecting to the MDM se
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDom: start  HTTP r
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDomNonComp: start
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- ===mdmFlowInfo===null,=====serve
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- QueryType is heartbeatQuery
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- using httpClient for http query
INFO  [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- GET: MDM Server URL: https://YOU
INFO  [Timer-12][[]] cisco.mnt.common.utility.AlarmMessageDiskQueue -::::- Inside dequeue
INFO  [Timer-12][[]] cisco.mnt.common.utility.AlarmMessageDiskQueue -::::- root exists
INFO  [Timer-12][[]] cisco.mnt.common.utility.AlarmMessageDiskQueue -::::- alarm.1692086243915 deleted
INFO  [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmServersCache -::::- MDM server - Status : Active,
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- Error message while connecting t
Connection Failed to the MDM server host - YOUR_ACCOUNT.jamfcloud.com, and port - 443 : Connection time
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDom: end  HTTP req
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDomNonComp: end  H
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- Exception occurred while co
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.api.MdmClient -::::- A connection timeout occurred. Check
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::- returning from the method : ca
  apiPath: null
  redirectUrl: null
  queryMaxSize: null
  apiVersion: null
  vendor: null
  productName: null
  productVersion: null
  COMMA: ,
  errorMsg: null
  errorOccurred: true
}
```

Dall'acquisizione dei pacchetti, esaminare le informazioni seguenti:

Traffico DNS: ISE esegue una query sull'istanza correlata a JAMF se si immette il nome host nella sezione di configurazione dell'integrazione. Se la risoluzione del nome host non è visibile, provare a utilizzare l'indirizzo IP. Questa opzione è disponibile per la configurazione al posto del nome host.

Source	Destination	Protocol	Length	Info
10.88.240.21	10.88.240.59	DNS	85	Standard query 0x5a75 A
10.88.240.21	10.88.240.59	DNS	85	Standard query 0x9f69 A
10.88.240.59	10.88.240.21	DNS	206	Standard query response
10.88.240.59	10.88.240.21	DNS	158	Standard query response

Traffico DNS in un flusso MDM

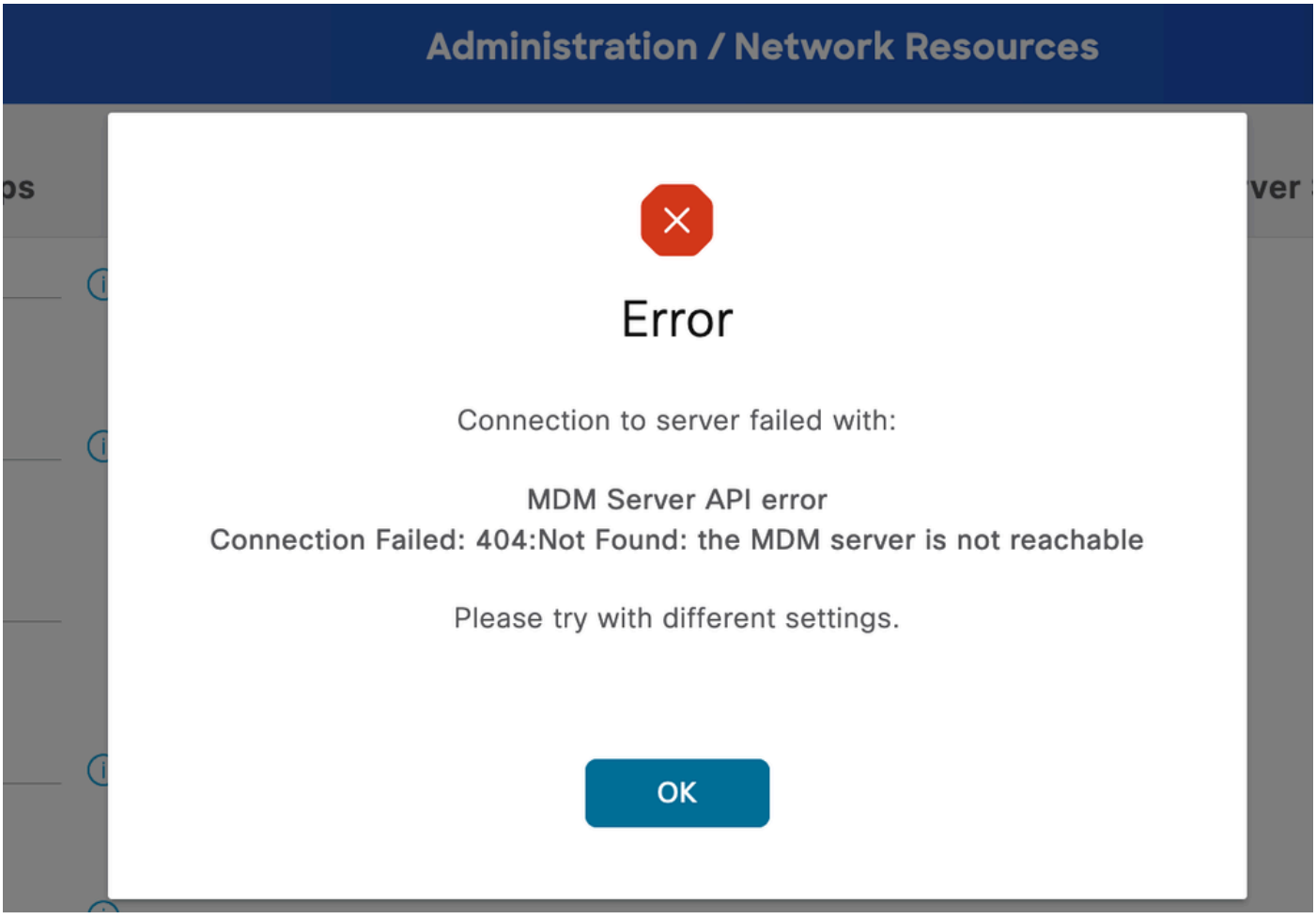
Ritrasmissioni nella porta di connessione MDM: se si esegue una query direttamente sull'indirizzo IP (specificato nella query DNS o nell'installazione di MDM), è possibile che vengano visualizzati i pacchetti SYN ripetuti. Ciò indica che non è disponibile alcun percorso diretto all'istanza JAMF o che un dispositivo esterno interferisce con le comunicazioni sulla porta 443.

Source	Protocol	Length	Info
10.88.240.21	TCP	74	22432 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=272773814 TSecr=0 WS=128
10.88.240.21	TCP	74	[TCP Retransmission] 22432 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=272774846 TSecr=0 WS=128
10.88.240.21	TCP	74	[TCP Retransmission] 22432 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=272776894 TSecr=0 WS=128

Esempio di timeout della connessione a MDM

Scenario 2. Connessione non riuscita: 404

Questo evento indica la presenza di connettività all'account JAMF configurato durante la configurazione del server MDM. Tuttavia, l'istanza indicata per la connessione non esiste o contiene un errore poiché non viene trovata.



Esempio di errore MDM 404

Vengono visualizzati i registri corrispondenti a questo evento:

```
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::::- inside the method : callMdmSer
TRACE [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- Inside MDMVerifyServer.veri
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- API version retrieved from
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- apiVersionSb : 3, mdmApiVer
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- MDM Rest API Server Query S
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- MDM Rest API Server Query P
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- 1. Connecting to the MDM se
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDom: start  HTTP r
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: start
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- ===mdmFlowInfo===null,=====serve
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- QueryType is heartbeatQuery
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- using httpClient for http query
INFO  [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- GET: MDM Server URL: https://YOU
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- Proxy Config in request  = [,PRO
INFO  [admin-http-pool37][[]] cpm.admin.infra.spring.ISEAdminControllerUtils -::admin:::- mapping path
INFO  [admin-http-pool37][[]] cpm.admin.infra.spring.ISEAdminControllerUtils -::admin:::- mapping path
INFO  [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmServersCache -::::::- MDM server - Status : Active,
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- Error message while connecting t
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDom: end  HTTP req
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: end  H
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- Exception occurred while co
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmClient -::::::- Connection Failed: 404:: the MDM serv
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::::- returning from the method : ca
  apiPath: null
  redirectUrl: null
  queryMaxSize: null
  apiVersion: null
  vendor: null
  productName: null
  productVersion: null
  COMMA: ,
  errorMsg: null
  errorOccurred: true
}
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmServersCache -::::::- mdm Guid: GUID is found in cac
```

L'acquisizione dei pacchetti fornisce ora una connessione HTTPS che contiene i dati dell'applicazione che vengono trasferiti tra il sito JAMF e il server ISE.

Source	Protocol	Length	Info
10.88.240.21	HTTP	183	CONNECT :443 HTTP/1.1
10.31.104.78	HTTP	105	HTTP/1.1 200 Connection established
10.88.240.21	TLSv1.2	419	Client Hello
10.31.104.78	TLSv1.2	213	Server Hello, Change Cipher Spec, Encrypted Handshake Message
10.88.240.21	TLSv1.2	72	Change Cipher Spec
10.88.240.21	TLSv1.2	111	Encrypted Handshake Message
10.88.240.21	TLSv1.2	349	Application Data
10.31.104.78	TLSv1.2	1024	Application Data

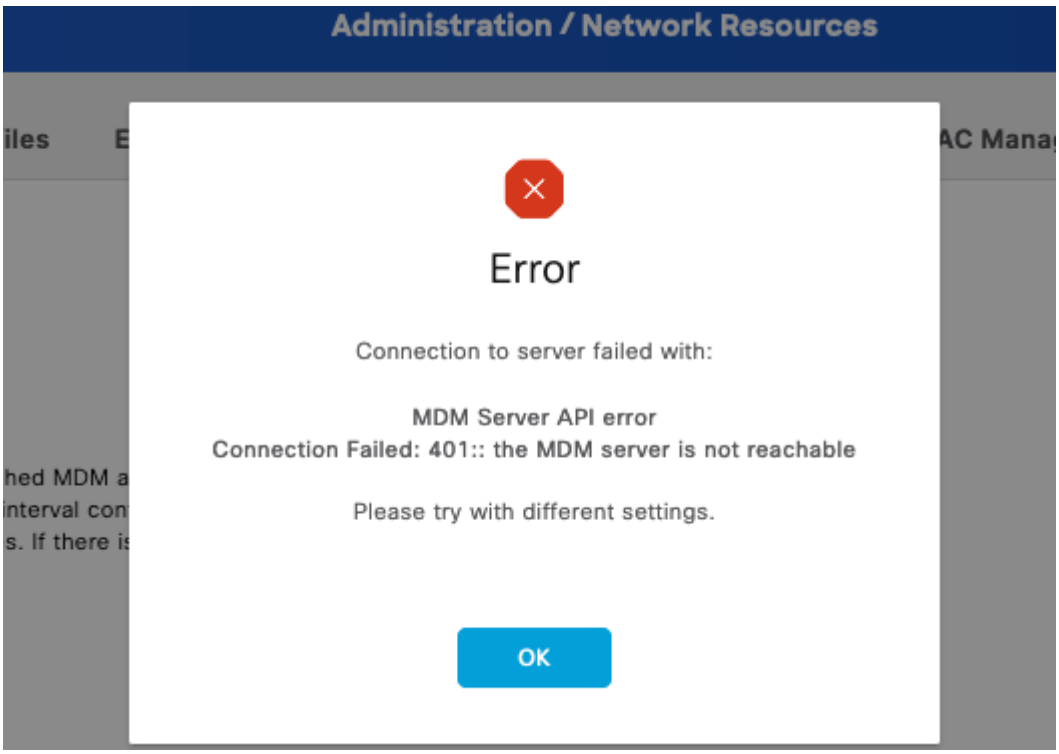
Pacchetti interessati dall'errore 404 MDM

Scenario 3. Connessione non riuscita: 401

Questo errore nella connessione indica un problema con l'utente che si sta distribuendo nell'installazione di MDM da integrare.

Verificare che l'utente:

- Esiste all'interno dell'account JAMF.
- Dispone dei privilegi appropriati per completare l'integrazione con ISE.
- e può essere utilizzato per eseguire l'autenticazione API (come descritto in precedenza in questa guida).



Codice di errore connessione MDM 401

L'accesso ad ISE indica questo comportamento:

```
INFO  [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- GET: MDM Server URL: https://YOUR
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- Proxy Config in request  = [,PROX
ERROR [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- Error message while connecting to
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDom: end  HTTP requ
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: end  HT
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- retry connecting using api v
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- MDM Rest API Server Query St
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- MDM Rest API Server Query PA
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- 2. On Error : re-connecting
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDom: start  HTTP re
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: start
```

```
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- ===mdmFlowInfo===null,=====server
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- QueryType is heartbeatQuery
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- using httpClient for http query -
INFO  [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- GET: MDM Server URL: https://YOUR
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- Proxy Config in request  = [,PROX
ERROR [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- Error message while connecting to
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDom: end  HTTP requ
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDomNonComp: end  HT
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- retry connecting using api v
```

L'acquisizione dei pacchetti rivela un comportamento simile a quello mostrato nell'immagine:

Source	Protocol	Length	Info
10.88.240.21	HTTP	183	CONNECT :443 HTTP/1.1
10.31.104.78	HTTP	105	HTTP/1.1 200 Connection established
10.88.240.21	TLSv1.2	419	Client Hello
10.31.104.78	TLSv1.2	213	Server Hello, Change Cipher Spec, Encrypted Handshake Message
10.88.240.21	TLSv1.2	72	Change Cipher Spec
10.88.240.21	TLSv1.2	111	Encrypted Handshake Message
10.88.240.21	TLSv1.2	349	Application Data
10.31.104.78	TLSv1.2	1071	Application Data
10.88.240.21	TLSv1.2	349	Application Data
10.31.104.78	TLSv1.2	1071	Application Data

Pacchetti MDM interessati dall'errore 401

Informazioni correlate

- Integrazione JAMF con ISE 2.X come MDM
- Risoluzione dei problemi e abilitazione dei debug su ISE
- Come abilitare i debug sulle versioni ISE 3.x.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).